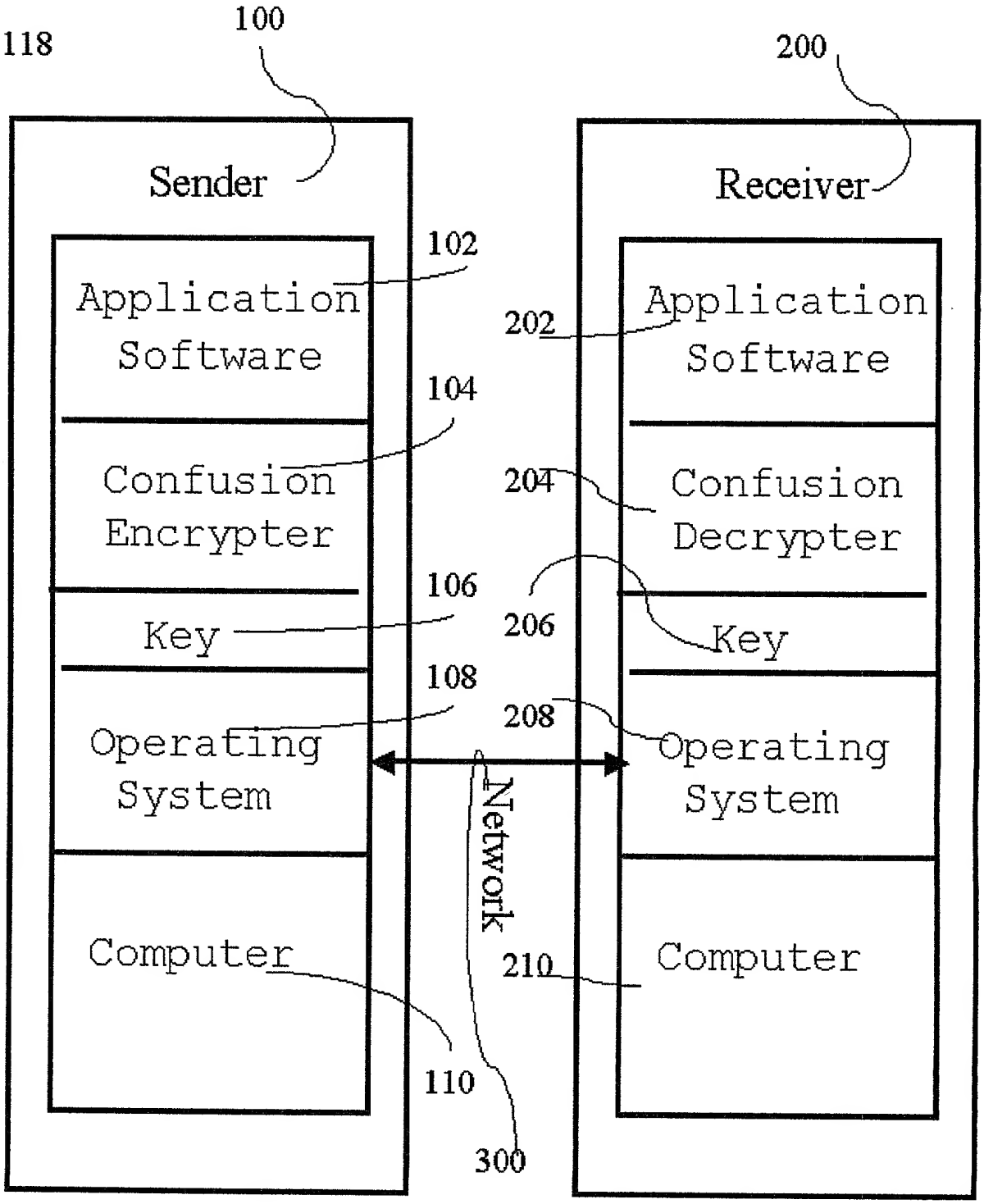
118
100
200
Sender
Receiver
102
Application Software
202
Application Software
104
Confusion Encrypter
204
Confusion Decrypter
106
Key
206
Key
108
Operating System
208
Operating System
Network
Computer
210
Computer
110
300

FIG.1

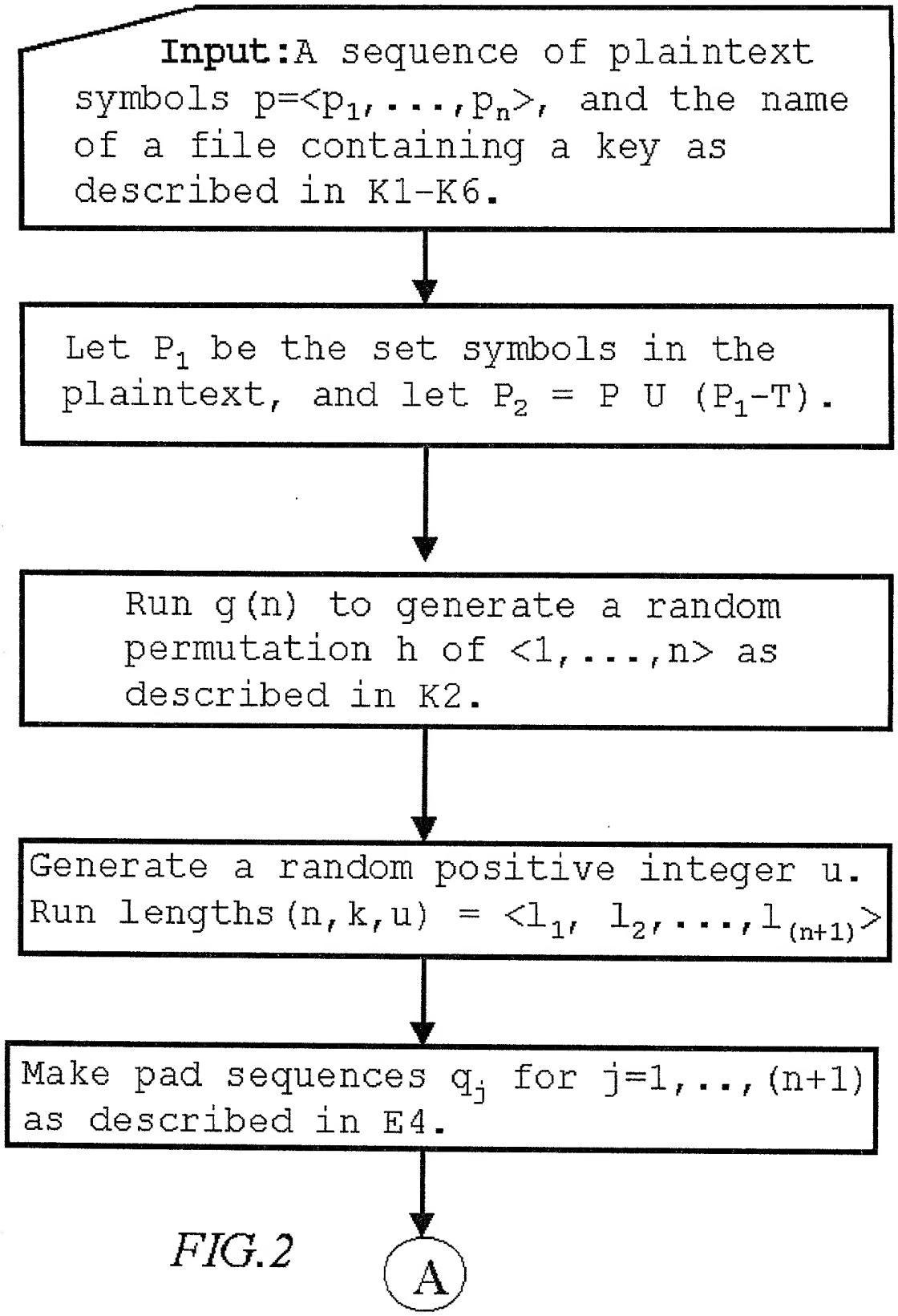

FIG.2

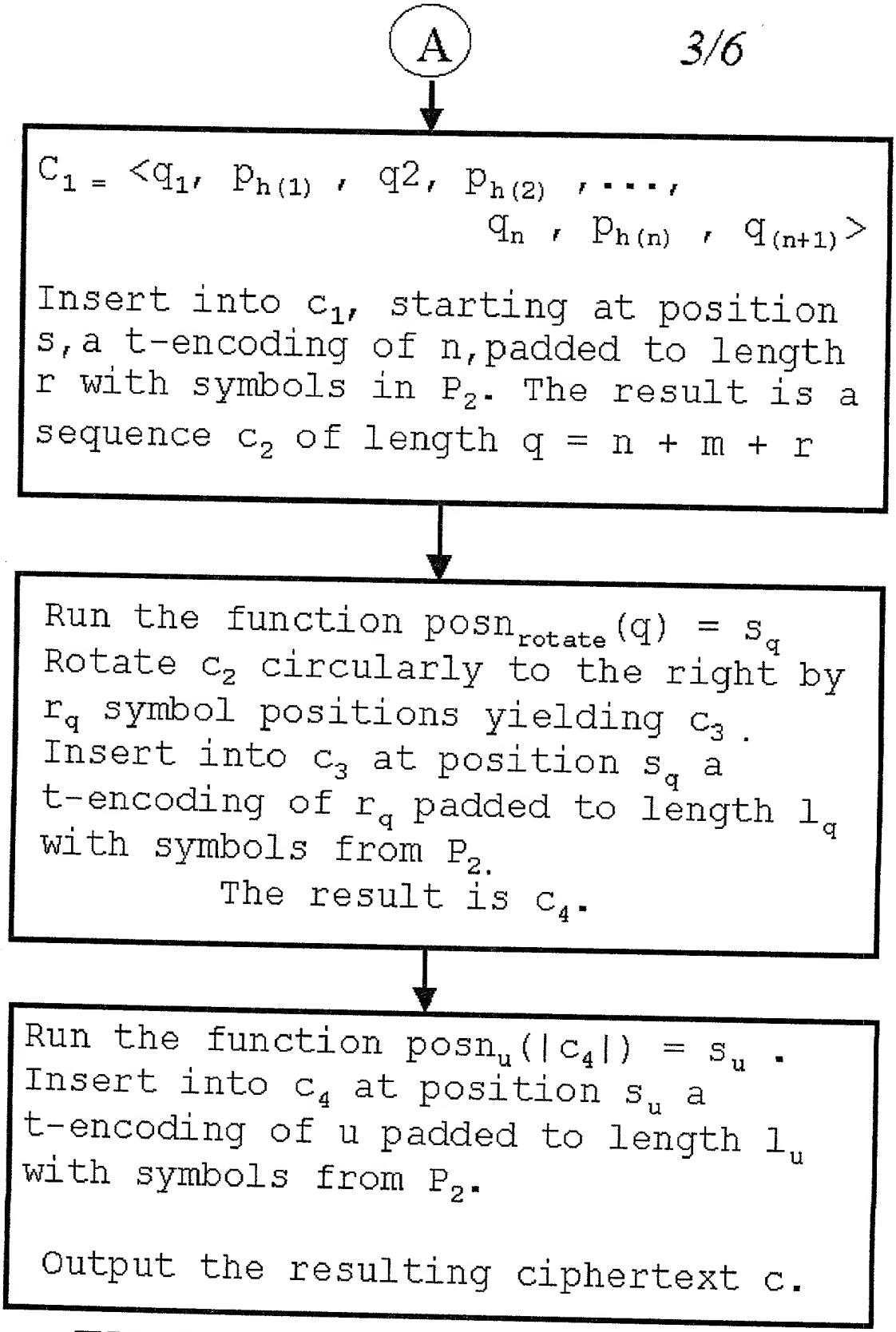

FIG.3

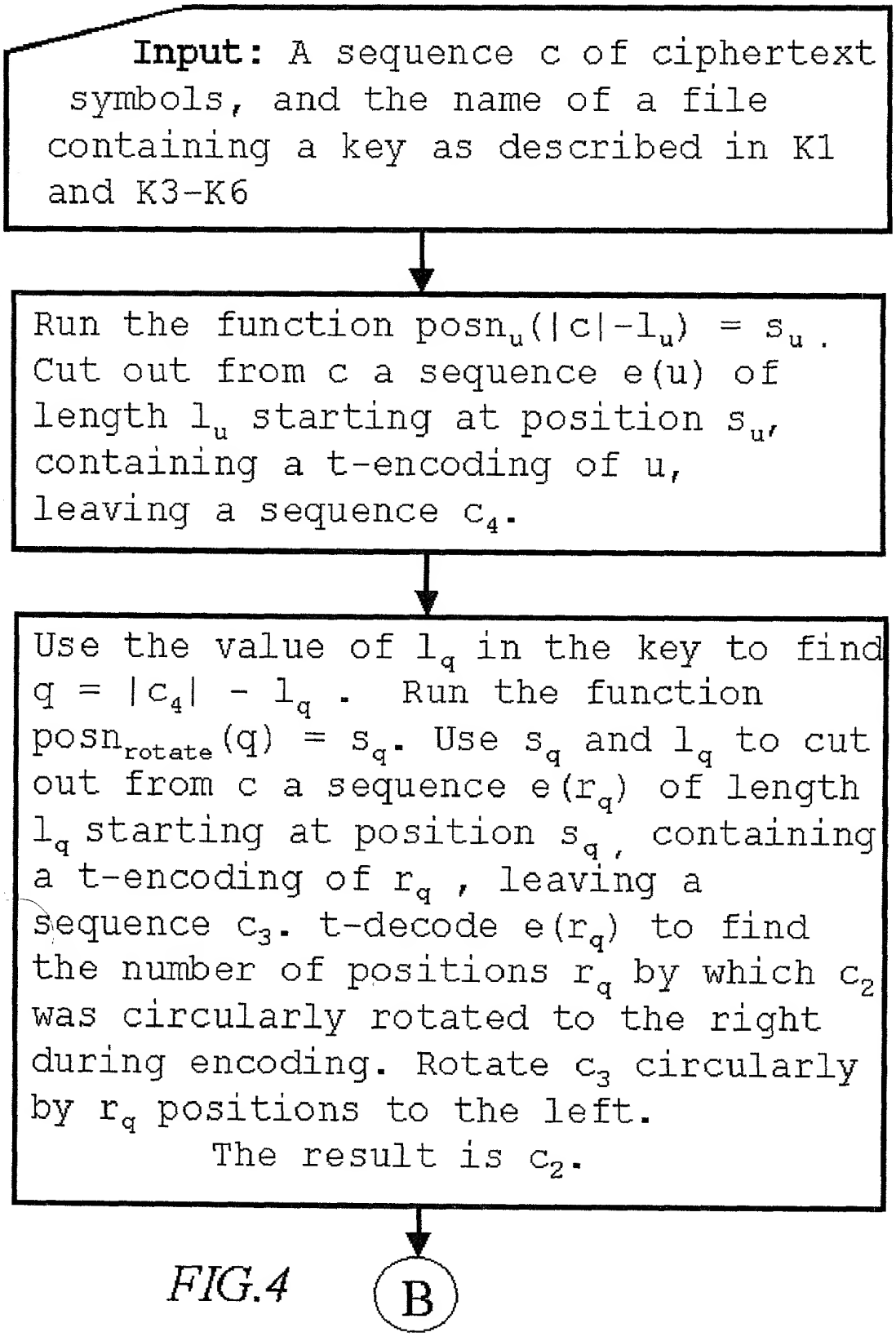
Input: A sequence c of ciphertext symbols, and the name of a file containing a key as described in K1 and K3-K6
Run the function $posn_u(|c|-l_u) = s_u$. Cut out from c a sequence e(u) of length l_u starting at position s_u, containing a t-encoding of u, leaving a sequence c_4.
Use the value of l_q in the key to find $q = |c_4| - l_q$. Run the function $posn_{rotate}(q) = s_q$. Use s_q and l_q to cut out from c a sequence $e(r_q)$ of length l_q starting at position s_q, containing a t-encoding of r_q, leaving a sequence c_3. t-decode $e(r_q)$ to find the number of positions r_q by which c_2 was circularly rotated to the right during encoding. Rotate c_3 circularly by r_q positions to the left.
The result is c_2.
B

FIG.4

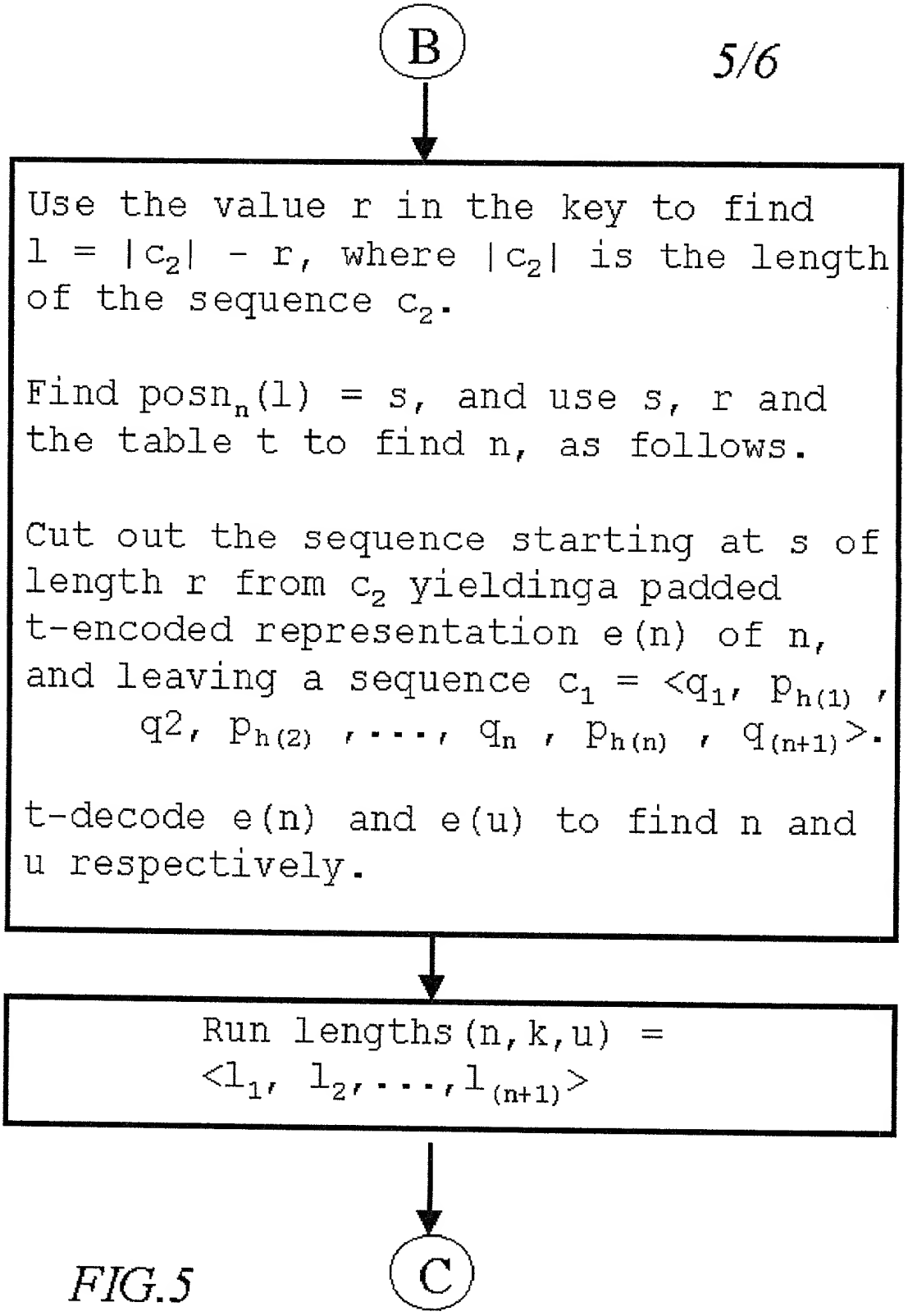
B
Use the value r in the key to find l = |c2| - r, where |c2| is the length of the sequence c2.
Find posn_n(l) = s, and use s, r and the table t to find n, as follows.
Cut out the sequence starting at s of length r from c2 yieldinga padded t-encoded representation e(n) of n, and leaving a sequence c1 = <q1, p h(1) , q2, p h(2) , ..., qn , p h(n) , q (n+1)>.
t-decode e(n) and e(u) to find n and u respectively.
Run lengths(n,k,u) = <l1, l2,...,l (n+1)>
C

FIG.5

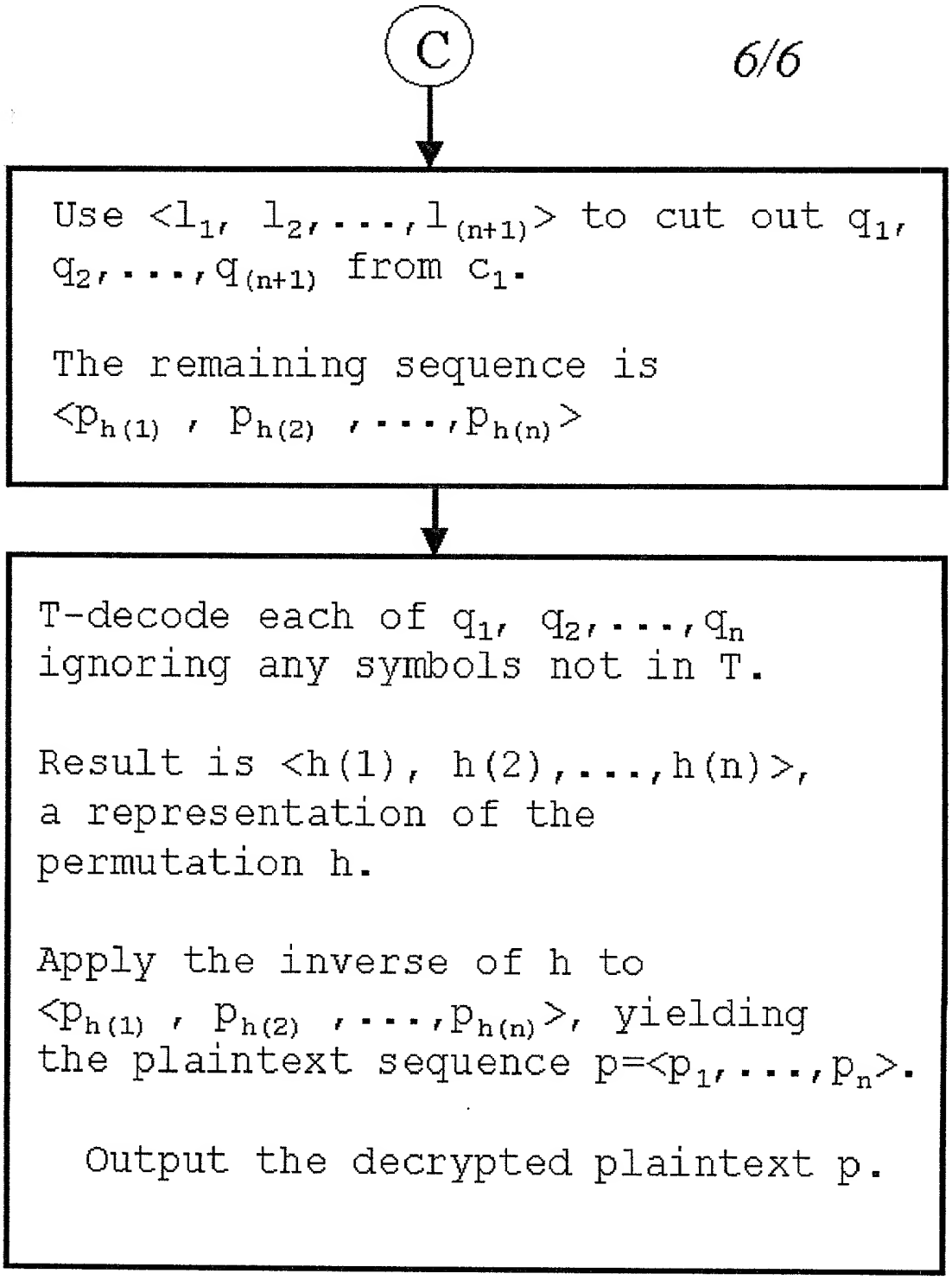

FIG.6